IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MONEYGRAM PAYMENT SYSTEMS, INC.,	§	
	§	
Plaintiff,	§	
	§	CIVIL ACTION NO.
v.	§	3:25-cv-00498-S
	§	
CAPGEMINI AMERICA, INC.,	§	
	§	**Oral Argument Requested**
Defendant.	§	
	§	

DEFENDANT CAPGEMINI AMERICA, INC.'S MOTION TO DISMISS PLAINTIFF MONEYGRAM PAYMENT SYSTEMS, INC.'S FIRST AMENDED COMPLAINT AND BRIEF IN SUPPORT THEREOF

Jeffrey M. Tillotson
State Bar No. 20039200
J. Austen Irrobali
State Bar No. 24092564
TILLOTSON JOHNSON & PATTON
1201 Main Street, Suite 1300
Dallas, Texas 75202
Telephone: (214) 382-3041
Facsimile: (214) 292-6564
Email: jtillotson@tillotsonlaw.com
airrobali@tillotsonlaw.com

Jenny H. Kim (*pro hac vice*)
Jack G. Tubio (*pro hac vice*)
BOIES SCHILLER FLEXNER LLP
55 Hudson Yards
New York, New York 10001
Telephone: (212) 446-2354
Email: jkim@bsfllp.com
jtubio@bsfllp.com

Counsel for Defendant Capgemini America, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Rules

Defendant Capgemini America, Inc. ("Capgemini") respectfully submits this memorandum in support of its motion to dismiss Plaintiff MoneyGram Payment Systems, Inc.'s ("MoneyGram") First Amended Complaint (ECF 17, hereinafter "FAC") pursuant to Federal Rule of Civil Procedure 12(b)(6).[1]

PRELIMINARY STATEMENT

This dispute arises from an alleged data incident (the "Data Incident") in which a third-party criminal actor (the "Criminal Third Party") gained access to MoneyGram's network and the personal data of its customers. In its original complaint (ECF 1, hereinafter "Complaint" or "Compl."), MoneyGram asserted contract claims against Capgemini, alleging that Capgemini was responsible for the Criminal Third Party accessing and disclosing the personal data of MoneyGram's customers. According to MoneyGram, the Criminal Third Party breached MoneyGram's network after contacting a service desk operated by Capgemini (the "Service Desk") to initiate a password reset by impersonating a former MoneyGram employee.

Capgemini then filed a motion to dismiss the Complaint that identified a fatal flaw with MoneyGram's claims: under the operative contracts, a Business Services Master Agreement ("MSA") and a related Statement of Work ("SOW"), Capgemini never had access to the personal data of MoneyGram's customers – and access to that personal data is a threshold requirement for Capgemini's liability for any data breach. (*See* ECF 11) Rather, under the SOW, Capgemini only operated a Service Desk for MoneyGram that provided the most basic IT services to MoneyGram employees.

[1] Pursuant to Local Rules 7.1(h)(i) and 7.2(e), Capgemini submits herewith an Appendix containing the Declaration of Jack G. Tubio and attached exhibits. Citations to "App." herein refer to pages in the Appendix. Unless otherwise specified, all emphases are added.

In response to Capgemini's motion to dismiss – and this specific argument – MoneyGram amended its Complaint to add allegations that Capgemini had access to, and disclosed, the personal data of MoneyGram ***employees***. In other words, MoneyGram's new argument is that Capgemini supposedly disclosed MoneyGram's employee data to the Criminal Third Party; with that data, the Criminal Third Party gained access to MoneyGram's network; and anything after that – including the Criminal Third Party's breach of MoneyGram's own security network – is Capgemini's fault. MoneyGram never identifies what specific employee data Capgemini disclosed, alleging only that a Capgemini employee "coached" the Criminal Third Party to the correct answer to an authentication prompt. (FAC ¶ 40) MoneyGram – which has reviewed all the call tapes and knows exactly what happened with respect to the Criminal Third Party – would have identified the disclosed employee data if it could have. But since no employee data was disclosed, the best it can do is allege "coaching."

In short, nothing in the FAC changes the reality of this case: in negotiating the MSA and the SOW, the parties allocated responsibility for security breaches based on what data a party controlled. As MoneyGram now concedes, Capgemini never controlled or had access to MoneyGram's customer's personal data, which is now the subject of at least nine data breach class actions (the "Customer Class Actions"). Allegations of "coaching" cannot change these express contract provisions.

Perhaps realizing the futility of its contract claims, MoneyGram's FAC also adds a claim for negligence. This claim, however, fails as a matter of law because Texas law does not permit a tort claim when the parties' relationship is governed by a contract. Because the FAC fails to state a claim upon which relief can be granted, it should be dismissed in its entirety.

PROCEDURAL HISTORY

On November 27, 2024, MoneyGram sent a demand letter to Capgemini, which is referenced in paragraph 40 of the Complaint and paragraph 67 of the FAC. (*See* App. 79-80) In that demand letter, MoneyGram notified Capgemini that MoneyGram's customers had filed nine lawsuits against MoneyGram based on the Data Incident, which disclosed the personal data of MoneyGram's customers. (*Id.*; *see* Compl. ¶ 40; FAC ¶ 67) The letter demanded that Capgemini indemnify MoneyGram for its liabilities arising from the Customer Class Actions. (*Id.*)

On February 27, 2025, MoneyGram filed its Complaint against Capgemini. Similar to its demand letter, the Complaint seeks to hold Capgemini responsible for damages MoneyGram has allegedly incurred in connection with the disclosure of MoneyGram's customer data following the Data Incident. (*See* Compl. ¶¶ 25, 31, 36) The Complaint alleged that Capgemini was responsible for these damages because the Service Desk had disclosed MoneyGram customers' personal data to the Criminal Third Party. (*Id.* ¶ 25) MoneyGram asserted claims against Capgemini for breach of contract, indemnification, and declaratory judgment.

On May 1, 2025, Capgemini filed its motion to dismiss MoneyGram's Complaint. (ECF 11) In its motion, Capgemini explained that it never had access to Customer Personal Data, as its role under the MSA and SOW was limited to providing a Service Desk to provide basic IT services to MoneyGram employees, not MoneyGram customers. (*See* ECF 11, pp. 13-17) Capgemini therefore could not have disclosed the personal data of MoneyGram customers and could not have breached the contractual provisions cited by MoneyGram. (*Id.*)

In response to this argument, MoneyGram amended its Complaint and filed the FAC on June 12, 2025. In the FAC, MoneyGram adds allegations that Capgemini had access to, and disclosed, the personal data of MoneyGram employees. (*See, e.g.*, FAC ¶¶ 17-22) The FAC also

asserts a negligence claim alleging that Capgemini breached a duty to exercise reasonable care over MoneyGram's data. (*Id.* ¶¶ 98-107) For the reasons discussed below, MoneyGram's allegations remain deficient, and its new negligence claim fails as a matter of law.

STATEMENT OF FACTS

I. MoneyGram Hired Capgemini To Provide A Service Desk For Its Employees

Capgemini is a global leader in technology services, offering a range of information technology and business solutions to clients worldwide. (FAC ¶ 2) Among its many services, Capgemini offers clients a "Service Desk," which is manned by Capgemini employees and provides IT support to a client's employees who contact the Service Desk. (*See id.* ¶ 16; *see also* SOW § 5.1, App. 53)

MoneyGram is a money transfer company that allows customers to send money. (FAC ¶ 1) On August 20, 2020, MoneyGram hired Capgemini to provide Service Desk services for MoneyGram employees. (*Id.* ¶¶ 15-16) To memorialize their agreement, the parties executed the MSA, a standard vendor contract providing generally that the parties "desire that [Capgemini] provide certain services to [MoneyGram]." (MSA at 1, App. 4) The MSA stated that the scope of Capgemini's work for the specific engagement would be "more fully described in a statement of work ('SOW') executed pursuant to this Agreement" (*id.*), which "shall include a description of the Services." (*Id.* at § 1.2(a), App. 5) Only one SOW was ever executed under the terms of the MSA. (*See* SOW at 1, App. 51)

Pursuant to the SOW, Capgemini's services were limited to "ongoing delivery and running of Service Desk Services." *(Id.* § 3, App. 53) Specifically, Capgemini was obligated to maintain and staff a Service Desk to address "Service Requests" (*id.* § 4(c), App. 53), which included "request[s] for information or advice, or for a standard change (a pre-approved change that is low

risk, relatively common and follows a procedure) or for access to an IT service." (*Id.* § 1 (definition of "Service Request"), App. 52) Notably, MoneyGram provided all of the "work instructions" (*see* FAC ¶¶ 39-40) for Capgemini's Service Desk employees to follow, including instructions relating to password resets. (SOW § 5.1.10.18; *see also id.* § 5.1.3) Further, all work done by Capgemini's Service Desk employees was performed on platforms, systems, and tools provided and maintained by MoneyGram, including the MoneyGram IT Services Management ("ITSM") ticketing tool (called Service Now), the Remote Connectivity Bomgar tool, and the Password Reset Console. (*Id.* § 5.1.10.9)

II. Capgemini's Services Did Not Involve Access To Customer Personal Data

MoneyGram contends that Capgemini is responsible for a Security Breach that resulted in the Customer Class Actions. Security Breaches are addressed in Exhibit D to the MSA, which is a Data Processing and Data Security Addendum (the "Data Security Addendum" or "Exhibit D") to the MSA. Exhibit D, by its terms, applies *only if* the services that Capgemini provided included the handling of "Customer Personal Data." (*See* DSA, App. 32-37; MSA § 5, App. 13) Customer Personal Data is defined narrowly:

> "Customer Personal Data" means any Personal Data which is provided to, or accessed by, [Capgemini] by or at the direction of [MoneyGram] ***and*** that is Processed by [Capgemini] on behalf of [MoneyGram].

(DSA § 1.2, App. 32) The term "Personal Data" within this definition means "any data that identifies, relates to, is capable of being associated with, or could reasonably be linked to an identified or identifiable natural person or household." (*Id.* § 1.7, App. 32)[2] Further, Capgemini's

[2] The term "Processing" is also defined:

> "Processing, Processes, Processed or Process" means any operation or set of operations which are performed on Personal Data or on sets of Personal Data,

potential liability for a "Security Breach" with respect to Customer Personal Data is limited to situations involving "Customer Personal Data transmitted, stored or otherwise processed on systems under the ***direct control*** of [Capgemini]." (*Id.* § 1.12, App. 33)

In its original Complaint, MoneyGram asserted that the term "Customer Personal Data" referred to the personal data of MoneyGram's customers. (*See* Compl. ¶¶ 16-18) This interpretation comported with MoneyGram's demand letter, which requested indemnification under the MSA for the Customer Class Actions, all of which assert claims for the disclosure of customer personal data. (*See* App. 79-80) However, Capgemini did not have direct control of MoneyGram's customers' personal data, and so, in the FAC, MoneyGram added allegations that: (a) MoneyGram's employees' personal data somehow falls within the scope of Customer Personal Data, (b) a Capgemini Service Desk employee's "coaching" of the Criminal Third Party somehow constituted disclosure of employee personal data, and (c) that coaching somehow makes Capgemini liable for the Customer Class Actions and everything that followed. (FAC ¶¶ 17-22, 40)

III. The Criminal Third Party, Not Capgemini, Breached MoneyGram's Security And Accessed Customer Data

As alleged in the FAC, on September 20, 2024, the Criminal Third Party contacted a Capgemini Service Desk employee and falsely claimed to be MoneyGram's then-former Chief Financial Officer. (FAC ¶ 39) The third party requested a password and multi-factor

---

> whether or not by automated means, such as, collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available, restricting, erasing, destroying Customer Personal Data.

(DSA § 1.9, App. 32)

authentication reset for the former CFO's employee account. (*Id.*) (For reasons not explained by MoneyGram, MoneyGram's former CFO still had an operating account at MoneyGram.) The FAC alleges that Capgemini had work instructions in place requiring identity authentication through multiple knowledge-based prompts and, in the event of a failed authentication, escalation to the employee's direct supervisor. (*Id.*) These allegations are consistent with Capgemini's contractual obligations under SOW Section 5.1.3(e), which requires Capgemini to follow the policies and criteria established by MoneyGram in addressing a Service Request (like a password reset), to reject any Service Requests if those policies and criteria cannot be followed, and to escalate such Service Requests to MoneyGram as required. (SOW § 5.1.3(e), App. 57) According to the FAC, however, Capgemini's Service Desk attendant allegedly did not follow MoneyGram's work instructions and "coached" the Criminal Third Party to the correct answer to the authentication question, and then proceeded to authorize the requested reset.[3] (FAC ¶ 40) Thereafter, the Criminal Third Party logged into the former CFO's account, somehow breached MoneyGram's security network, and obtained MoneyGram's customers' personal data. (*Id.* ¶ 47)

IV. The Customer Class Actions And MoneyGram's Demand For Indemnity

The FAC alleges that "MoneyGram launched an investigation" "[i]mmediately upon discovering the Data Incident" on September 20, 2024. (FAC ¶ 51) This investigation allegedly

[3] MoneyGram alleges that, upon information and belief, a threat actor breached Capgemini's systems on September 9 and accessed MoneyGram's employees' personal data, which then allowed the Criminal Third Party to access MoneyGram's systems on September 20, 2024. (FAC ¶ 35) These allegations are sheer speculation and are contradicted by MoneyGram's admission (confirmed by SOW § 5.1.10.9) that Capgemini's Service Desk services were provided on MoneyGram's IT services management (or "ITSM") platforms. (FAC ¶¶ 16, 19) Even assuming that Capgemini suffered a data breach on September 9, none of MoneyGram's data was stored on Capgemini's systems as all of Capgemini's work for MoneyGram was conducted on MoneyGram's ITSM platforms. (*See id.*; SOW § 5.1.10.9, App. 60)

involved MoneyGram "completely shut[ting] down its entire global payments network for approximately six days," "coordinat[ing] with U.S. law enforcement," and "hir[ing] an external cybersecurity technology consultant, a law firm, and several other service providers to investigate the Data Incident." (*Id.* ¶¶ 51, 62)

Thereafter, "numerous lawsuits, including putative class actions, [were] filed against MoneyGram in the United States and Canada relating to and seeking damages arising out of the Data Incident." (*Id.* ¶ 63) According to the FAC, "MoneyGram has incurred and continues to incur legal expenses, including attorneys' fees, to defend against these lawsuits." (*Id.*) On November 27, 2024 – shortly after the ninth class action lawsuit was filed and over two months after the Data Incident – MoneyGram sent the demand letter to Capgemini, which sought indemnification for any damages and losses it has suffered, continues to suffer, and may suffer as a result of the Customer Class Actions. (*Id.* ¶ 67; *see* App. 79-80)

On October 3, 2024, MoneyGram also sent a preservation notice to Capgemini. (FAC ¶ 55; *see* App. 73-74) Although MoneyGram suggests that Capgemini's response to the preservation notice was deficient (FAC ¶ 57), Capgemini responded to MoneyGram's preservation notice on October 31, 2024, once again providing recordings of calls to the Service Desk and other documents, and noting that Capgemini employees no longer had access to MoneyGram platforms where all other relevant documents were maintained. (*See* App. 76)

LEGAL STANDARD

Under Rule 12(b)(6), a complaint must be dismissed when it fails to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). To survive dismissal, the FAC must contain "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is plausible when it contains "factual content that allows the

court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). While the Court must accept well-pleaded facts as true, the Court does not accept as true "conclusory allegations, unwarranted factual inferences, or legal conclusions." *Ferrer v. Chevron Corp.*, 484 F.3d 776, 780 (5th Cir. 2007) (quotations omitted). A plaintiff must provide "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555.

On a motion to dismiss, the Court may consider "documents incorporated into the complaint by reference." *Funk v. Stryker Corp.*, 631 F.3d 777, 783 (5th Cir. 2011). This includes documents that "are referred to in the plaintiff's complaint and are central to [its] claim," such as the MSA, the SOW, and MoneyGram's pre-suit letters. *Collins v. Morgan Stanley Dean Witter*, 224 F.3d 496, 498-99 (5th Cir. 2000). If these documents contradict the allegations in the complaint, the documents control. *Carter v. Target Corp.*, 541 F. App'x 413, 417 (5th Cir. 2013).

When enforcing a contract, courts "must give effect to the parties' intentions, as expressed in their agreement" by "giv[ing] a contract language its plain, grammatical meaning." *Mosaic Baybrook One, L.P. v. Simien*, 674 S.W.3d 234, 257 (Tex. 2023), *reh'g denied* (Sept. 29, 2023). "[C]ourts must give effect and purpose to each word in a contract," *Tennessee Gas Pipeline Co. v. FERC*, 17 F.3d 98, 104 (5th Cir. 1994) (citation omitted), and "may not rewrite a contract under the guise of interpretation," *Sundown Energy LP v. HJSA No. 3, Ltd. P'ship*, 622 S.W.3d 884, 889 (Tex. 2021).

ARGUMENT

I. Capgemini Has No Liability For The Data Incident And Customer Class Actions

To plead a breach of contract claim, a plaintiff must allege "(1) the existence of a valid contract; (2) performance or tendered performance by the plaintiff; (3) breach of the contract by

the defendant; and (4) damages to the plaintiff resulting from that breach." *Gonzales v. Columbia Hosp. at Med. City Dallas Subsidiary LP.*, 207 F. Supp. 2d 570, 575 (N.D. Tex. 2002). Here, the MSA and SOW expressly provide that Capgemini is not responsible for data it does not control. As MoneyGram concedes, Capgemini never controlled MoneyGram's customers' personal data, which was released by the Criminal Third Party and is the subject of the Customer Class Actions.

1. Capgemini Had No Access To, Or Control Of, MoneyGram's Customers' Personal Data

In MoneyGram's original Complaint, MoneyGram alleged that Capgemini's Service Desk employee allegedly failed to follow proper multi-factor authentication protocols and allowed the Criminal Third Party to reset MoneyGram employees' user accounts. (Compl. ¶¶ 26-27) MoneyGram then alleged that the Criminal Third Party ultimately gained access to MoneyGram's network and obtained certain data belonging to MoneyGram customers that was stored on the network (*id.* ¶ 31), and that disclosure of MoneyGram's customer data caused MoneyGram damages for which it sought indemnification. (*Id.* ¶ 36) Notably, the Complaint did not allege that Capgemini's Service Desk employees had access to MoneyGram's customers' personal data or disclosed any such data to a third party – nor could it. As detailed above, Capgemini's entire engagement was responding to routine MoneyGram employee IT requests through a Service Desk. (*See* pp. 4-6, *supra*)

In the FAC, MoneyGram still alleges that Capgemini's Service Desk employee allegedly failed to follow MoneyGram's authentication protocols and allowed the Criminal Third Party to reset MoneyGram employee's user accounts. (FAC ¶¶ 39-40) MoneyGram also still alleges that it was the Criminal Third Party that gained access to MoneyGram's network and obtained MoneyGram's customer data. (*Id.* ¶ 47) And MoneyGram still alleges that it was damaged by the disclosure of MoneyGram's ***customers'*** personal data – and seeks indemnification for those

damages. (*See id.* ¶¶ 3, 47-48, 63, 83) In fact, the only substantive difference between the Complaint and the FAC is that MoneyGram now also alleges that Capgemini is liable for the damages caused by the disclosure of MoneyGram's ***customers'*** personal data because Capgemini allegedly had access to and disclosed MoneyGram's ***employee*** data when a Capgemini Service Desk employee allegedly "coached" the Criminal Third Party to the right answer to an authentication question.[4] (*Id.* ¶ 40) In doing so, MoneyGram effectively concedes that Capgemini never had access to MoneyGram's customers' personal data.

Based on these allegations, MoneyGram alleges breaches of Sections 2.3(a), 2.3(c), 2.3(d), 6.1, and 7.1 of MSA Exhibit D or the Data Security Addendum. Despite MoneyGram's artful pleading, it is clear from the express language of the agreements that MSA Exhibit D does not apply to personal data of MoneyGram's employees (and certainly does not include an employee's answers to authentication prompts).

2. There Was No Security Breach Because Capgemini's Work Under The Agreements Took Place On MoneyGram's Own Systems And Platforms

Section 5.1.10.9 of the SOW provides that all the programs and platforms necessary for Capgemini to perform the Service Desk services, including licenses and accesses to MoneyGram's "ITSM ticketing tool (Service Now), Remote Connectivity Bomgar tool, [and] Password Reset Console" would be provided and maintained by MoneyGram. (SOW § 5.1.10.9, App. 60) Indeed, SOW Section 5.1.10, which provides "[MoneyGram's] Responsibilities and Service Desk assumptions," makes clear that MoneyGram had control over *all* the systems and platforms on

[4] That MoneyGram has manufactured an attempt to fix the deficiencies in its Complaint is evidenced by MoneyGram's November 27, 2024 demand letter to Capgemini, which only identified the disclosure of MoneyGram's *customer* data as the basis for MoneyGram's demand for indemnification. (App. 79-80)

which Capgemini performed the Service Desk services. (*See, e.g., id.* § 5.1.10.9, App. 60; § 5.1.10.14, App. 60 (MoneyGram is responsible for configuration of the ticketing tool); § 5.1.10.15, App. 60 (MoneyGram is responsible for configuration of reporting module); § 5.1.10.17, App. 60 (MoneyGram is responsible for all knowledge in Service Now platform); § 5.1.10.18, App. 60 (MoneyGram is responsible for all knowledge related to Service Desk activities being available via the Ticketing tool)).

MoneyGram concedes in the FAC that Capgemini's work under the relevant agreements was conducted on MoneyGram's ITSM platforms. (FAC ¶¶ 16, 19) As noted by Capgemini's in-house counsel in her response to MoneyGram's preservation notice, Capgemini could not even access relevant records regarding its work for MoneyGram after MoneyGram terminated its contract with Capgemini because everything had been "maintained exclusively on the MoneyGram platforms, including Service Now, to which [Capgemini's] employees no longer ha[d] access." (App. 76)

However, for disclosure of Customer Personal Data to be considered a Security Breach under the Data Security Addendum, the Customer Personal Data at issue must be "transmitted, stored or otherwise processed on systems under the ***direct control*** of [Capgemini]." (DSA § 1.12, App. 33) Because – as set forth in the SOW and conceded by MoneyGram – Capgemini never had direct control of any of the systems on which it conducted its Service Desk services, there was no Security Breach and MoneyGram's claims for breach of Section 7.1 of the Data Security Addendum and for indemnification under MSA Section 8.2(iii) and DSA Section 9(iii) fail.[5]

[5] MoneyGram cites Sections 4.1 and 5 to assert that the MSA contemplated MoneyGram providing access to MoneyGram employee personal data to Capgemini (*see* FAC ¶¶ 18-19), but in doing so, MoneyGram conveniently ignores the word "may" in both sections. (*See* MSA §§ 4.1, 5, App. 10,

3. Capgemini Could Not Have Breached Section 6.1 Because It Had No Control Over The Controls, Policies, Criteria, Platforms Or Systems Under Which It Operated

Similarly, because Capgemini worked exclusively on MoneyGram's platforms (as detailed above), and MoneyGram provided all of the criteria, policies, "knowledge," and "Knowledge Articles" (defined as "a document within the [MoneyGram] ticketing tool that provides instructions for the Service Desk to resolve Incidents and Service Requests") that Capgemini was instructed to follow in performing its Service Desk services, Capgemini could not have breached MSA Exhibit D Section 6.1. (*See* SOW § 1, App. 51 (defined terms); § 5.1.10.8, App. 60 (MoneyGram to configure the MoneyGram ticketing tool to enable Capgemini's Service Desk to perform Service Desk services, including the Knowledge, Incident and Service Requests and MGI Survey modules and a list of MoneyGram employee details and templates); § 5.1.10.9, App. 60 (MoneyGram to provide all programs and tools for Capgemini to perform the Service Desk services); § 5.1.10.14, § 5.1.10.15, § 5.1.10.17, and § 5.1.10.18, App. 60 (MoneyGram to provide all "knowledge" and configure all systems for Capgemini to perform Service Desk services)).

Indeed, Section 6.1 of the Data Security Addendum illustrates why the entirety of Exhibit D simply does not apply to the MoneyGram-Capgemini relationship. It provides:

> [Capgemini] shall implement appropriate technical and organizational measures to protect Customer Personal Data from unauthorized access, acquisition, or disclosure . . . that are no less rigorous accepted industry practices, and all such safeguards . . . will comply with Data Protection Laws. . . . These safeguards shall include, but are not limited to: (a) pseudonymization and encryption of Customer Personal Data; (b) the ability to maintain the on-going confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to

13) As noted in Capgemini's first motion to dismiss, the permissive "may" language simply reflects that such data could be involved in some engagements under the MSA, but does not establish that it was involved here – which it was not. (ECF 11 at p. 4 n.2) As the SOW makes clear, Capgemini was never hired by MoneyGram to handle Customer Personal Data. (*See* pp. 4-7, *supra*)

> restore the availability and access to Customer Personal Data in a timely manner . . .; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures. . . .

(DSA § 6.1, App. 36) As MoneyGram provided, controlled and configured all the systems and platforms on which Capgemini performed the Service Desk services, and provided all the criteria, models, policies, and instructions that Capgemini was required to follow in performing its services, it would have been impossible for Capgemini to provide any of the safeguards listed in Section 6.1. *See Guzman v. Acuna*, 653 S.W.2d 315, 319 (Tex. App. 1983) ("It is a basic tenet of contract law that a contract should be construed in such a manner as to render performance possible rather than impossible.") Again, Capgemini was only retained to provide Service Desk services and had no access to, or ability to control or safeguard, Customer Personal Data. Therefore, the Data Security Addendum does not apply.

For these same reasons, MoneyGram cannot allege a breach of Sections 2.3(a), (c), and (d) of the Data Security Addendum. Moreover, the FAC contains no factual allegations showing that Capgemini accessed, processed, or disclosed any data in a manner that would trigger a breach of those contractual provisions. It does not even identify what employee data was allegedly disclosed. The central allegation – that the Service Desk employee coached the Criminal Third Party to the correct answer to the authentication prompt and then reset that former employee's credentials (FAC ¶ 40) – is not the disclosure of even employee data, and certainly, is not the disclosure of MoneyGram's Customer Personal Data for which MoneyGram is seeking relief.

4. MoneyGram's "Coaching" Allegations Cannot Create Liability

As noted, in an effort to avoid Capgemini's lack of responsibility for MoneyGram's customer personal data, MoneyGram now alleges that Capgemini disclosed *employee* personal data. Specifically, MoneyGram alleges that Capgemini provided certain undefined employee

personal data to the Criminal Third Party by "coaching" him on an authentication prompt (*id.*), and as a result – and after a round-about "but for" causal path – Capgemini is liable for everything after that alleged coaching. However, these allegations fail to fix MoneyGram's breach claims for at least two reasons: (1) MoneyGram does not, because it cannot, identify any employee data that Capgemini actually controlled and released, and (2) MoneyGram is suing for released customer data – not released employee data.

Indeed, the FAC refers to, but fails to attach, MoneyGram's November 27, 2024 demand letter to Capgemini. (*Id.* ¶ 67) Why? Because it does not support MoneyGram's new "employee"-based theory. That letter refers only to the Customer Class Actions, which are based solely on released customer data. (App. 79-80) Nothing about MoneyGram's employees' data is mentioned in that letter or any of the Customer Class Actions. (*See id.*)

Once again, Capgemini was engaged to provide routine IT assistance through the Service Desk, not Processing of MoneyGram Customer Personal Data under the Data Security Addendum. MoneyGram's attempt to transform the limited services the Service Desk provided into broad liability for a cybersecurity breach is contradicted by the express language of the SOW, which makes clear that Capgemini was engaged to provide only services through the Service Desk. *See Campbell v. DLJ Mortg. Cap., Inc.*, 628 F. App'x 232, 234 (5th Cir. 2015) ("To the extent that the contracts conflict with [the plaintiff's] allegations, the contracts control."); *Carter*, 541 F. App'x at 417 (refusing to accept as true factual allegations that were contradicted by plaintiff's EEOC charging documents, which defendant had attached to its motion to dismiss).

Under the MSA and SOW, MoneyGram retained responsibility for securing its own systems and its own customers' personal data. Accepting MoneyGram's reframed theory would ignore the bargain the parties struck and stretch liability beyond the scope of their contract. *See*

Paso Del Norte Motors, LP v. Tri Star Partners, LLC, 2015 WL 13778413, at *6 (W.D. Tex. Sept. 3, 2015) ("[C]ontracting parties are free to structure their contractual undertaking and allocate risk as they see fit. The role of courts is not to protect parties from their own agreements, but to enforce contracts that parties enter into freely and voluntarily." (cleaned up)).

5. The FAC's Breach Of Contract Claim Also Fails For Lack Of Causation

MoneyGram's breach of contract claim must also be dismissed because it fails to plausibly allege a causal link between Capgemini's conduct and the damages it seeks. The FAC alleges at least two very real intervening causes: the involvement of a Criminal Third Party and the breach of MoneyGram's own internal security protocols and network. Under Texas law, "the absence of a causal connection between the alleged breach [of contract] and the damages sought will preclude recovery." *AZZ Inc. v. Morgan*, 462 S.W.3d 284, 289 (Tex. App.—Fort Worth 2015). Further, Texas courts have repeatedly held that criminal conduct is an intervening cause. *See, e.g., Urbach v. United States*, 869 F.2d 829, 833 (5th Cir. 1989) ("Texas cases also hold that an intervening criminal act will break the chain of causation.").

II. Because Capgemini Did Not Breach Any Obligations To MoneyGram, MoneyGram Is Not Entitled To Indemnification

MoneyGram's claim for indemnification under Section 8.2 of the MSA and Section 9 of the Data Security Addendum also fails.

Texas courts "impose a strict construction upon [the intent of the parties to an indemnity agreement] to prevent the indemnity obligation from being broadened beyond the terms of the agreement." *McClane v. Sun Oil Co.*, 634 F.2d 855, 859 (5th Cir. 1981) (citing *Sun Oil Co. (Delaware) v. Renshaw Well Serv., Inc.*, 571 S.W.2d 64, 68 (Tex. App.—Tyler 1978, writ ref'd n.r.e.)); *see also* 14 Tex. Jur. 3d Contribution, Etc. § 17 ("The nature of an indemnitor's liability is to be determined by the provisions of the indemnity contract."). "[I]ndemnity agreements are

strictly construed in favor of the indemnitor, and the indemnity must be clearly expressed." *Marathon E.G. Holding Ltd. v. CMS Enterprises Co.*, 597 F.3d 311, 317 (5th Cir. 2010). The terms of an indemnity "cannot be extended by construction or implication beyond its plain terms." *Smith v. Scott*, 261 S.W. 1089, 1089 (Tex. Civ. App.—Amarillo 1924, no writ).

MoneyGram first alleges that it is entitled to indemnification under Section 8.2(iii) of the MSA and Sections 9(i) and 9(ii) of the Data Security Addendum, for alleged "unauthorized Processing of Customer Personal Data" and "breach of the Data Security Addendum." (FAC ¶¶ 90-92) [6] However, as explained above, MoneyGram fails to allege any breach of the Data Security Addendum because MoneyGram controlled, configured and maintained the systems on which Capgemini provided the Service Desk services and further provided the specific criteria, policies, protocols and instructions that Capgemini was required to follow in addressing any Service Request. (*See* pp. 9-16, *supra*) Further, MoneyGram fails to allege any disclosure of any Customer Personal Data in its FAC. The closest that MoneyGram gets is an allegation that a Capgemini Service Desk employee coached a caller to the correct answer to an authentication prompt. (FAC ¶ 40) But coaching is not disclosing.

Finally, MoneyGram is seeking indemnity for the disclosure of MoneyGram's customers' data; this has been clear since MoneyGram sent its November 27, 2024 demand letter and is undisputed. (*See* FAC ¶ 67; App. 79-80) As MoneyGram now concedes, Capgemini never accessed, processed, or disclosed any of MoneyGram's Customer Personal Data, and thus, MoneyGram is not entitled to indemnification from Capgemini. (*See* pp. 10-11, *supra*)

[6] MoneyGram does not allege an indemnification claim under Section 8.2(i), which concerns "breach of the Indemnifying Party's representations and warranties under the [MSA]" (MSA § 8.2(i), App. 16), or Section 8.2(ii), which concerns "gross negligence or willful misconduct of the Indemnifying Party" (MSA § 8.2(ii), App. 16).

MoneyGram's claims for indemnity under Section 8.2(iii) of the MSA and Sections 9(i) and 9(ii) of the Data Security Addendum should be dismissed.

MoneyGram also alleges that it is entitled to indemnification under Section 9(iii) of the Data Security Addendum because there was "a Security Breach." (FAC ¶¶ 90, 93) This claim also fails for the reasons discussed in Part I.2 above. (*See* pp. 11-12, *supra*)

III. In The Alternative, MoneyGram's Claim Should Be Limited By The One Million Dollar Cap Found In MSA Section 7.2

MoneyGram's tortured attempt to shove the MoneyGram-Capgemini relationship into the Data Security Addendum is for one reason only: to avoid the limitation of liability clause in Section 7.2 of the MSA, which limits total damages to one million dollars and precludes the recovery of indirect, special, incidental, punitive, or consequential damages. (MSA § 7.2, App. 15) Because Section 7.2 carves out breaches of the Data Security Addendum (*id.*), MoneyGram crafted its breach claims as claims for breach of the Data Security Addendum.

MoneyGram's own allegations make clear, however, that Capgemini's wrongful conduct is limited to Capgemini allegedly "fail[ing] to verify the caller" to the Service Desk (FAC ¶¶ 42-44) and failing to follow MoneyGram's "work instructions" regarding the authentication of callers. (FAC ¶¶ 39-40) Even if true (which it is not), this would be a breach of Section 5.1.3(e) of the SOW, which provides that, if Capgemini cannot properly authenticate a caller, then Capgemini should reject the caller's request, and if necessary, escalate to MoneyGram the caller's request. (SOW § 5.1.3(e), App. 57) If the Court does not dismiss MoneyGram's breach of contract claims outright, MoneyGram's claims should be characterized for what they really are – a breach of SOW Section 5.1.3(e) – and subject to MSA Section 7.2's one million dollar limitation on liability. *See Moon Soo Kim v. Stanley Convergent Sec. Sols., Inc.*, 2013 WL 1715789, at *2 (N.D. Tex. Apr. 19, 2013) (Texas law "unequivocally establish[es] that [liability limiting] provisions are

presumptively valid and supported by public policy"); *Cont'l Holdings, Ltd. v. Leahy*, 132 S.W.3d 471, 475-77 (Tex. App. 2003) (liability limiting provision "unambiguously precludes the recovery of" damages sought by plaintiff).

Here, it is the specific provision of the SOW – not the general terms of the Data Security Addendum – that defines Capgemini's conduct and responsibilities with respect to the Service Desk. Because Section 5.1.3(e) of the SOW expressly addresses how Capgemini must handle Service Requests that do not conform to MoneyGram policy (SOW § 5.1.3(e), App. 57), it must control. *See Mosaic*, 674 S.W.3d at 257 (affirming Texas' "long-established precedent" that "a specific contract provision controls over a general one" (citation omitted)).

IV. MoneyGram's Negligence Claim Fails for Additional Reasons

1. The Economic Loss Rule Bars the Negligence Claim

The FAC also brings a negligence claim based on Capgemini's alleged failure to exercise reasonable care over MoneyGram's data. Because it seeks to recover in tort for purely economic damages, MoneyGram's repackaged claim is barred by the economic loss doctrine.

"The Texas Supreme Court has unequivocally adopted a broad interpretation of the economic loss rule." *Mem'l Hermann Healthcare Sys. Inc. v. Eurocopter Deutschland, GMBH*, 524 F.3d 676, 678 (5th Cir. 2008) (*citing Jim Walter Homes, Inc. v. Reed*, 711 S.W.2d 617, 618 (Tex. 1986) (affirming dismissal of negligence claim). Under this rule, "if a plaintiff only seeks to recover for the loss or damage to the subject matter of a contract, he cannot maintain a tort action against a defendant." *Sterling Chemicals, Inc. v. Texaco Inc.*, 259 S.W.3d 793, 796 (Tex. App. 2007) (*citing Sw. Bell Tel. Co. v. DeLanney*, 809 S.W.2d 493, 494 (Tex. 1991). In other words, "a duty in tort does not lie when the only injury claimed is one for economic damages recoverable under a breach of contract claim." *Id.*; *see Mem'l Hermann*, 524 F.3d at 678. Courts in this district

routinely apply the economic loss rule to dismiss negligence-based claims. *See, e.g., Johnson v. Wells Fargo Bank, NA*, 999 F. Supp. 2d 919, 930-31 (N.D. Tex. 2014); *Miller v. CitiMortgage, Inc.*, 970 F. Supp. 2d 568, 586-87 (N.D. Tex. 2013).

Texas courts weigh two considerations to determine whether a Plaintiff may bring an additional negligence claim where there is an underlying claim for breach of contract: "First, a court should examine the faulted conduct to determine if it violates duties imposed by law, independent of those duties imposed by the contract. Next, it should examine the nature of the alleged injury, recognizing that '[w]hen the injury is only the economic loss to the subject of a contract itself the action sounds in contract alone.'" *Heller Financial, Inc. v. Grammco Computer Sales, Inc.,* 71 F.3d 518, 528 (5th Cir. 1996) (quoting *Jim Walter Homes*, 711 S.W.2d at 618).

Here, MoneyGram fails to allege any duties underlying its negligence claim that are independent of those underlying its breach of contract claim. MoneyGram's allegation that Capgemini breached its "duty to exercise reasonable care over the personal data it stored and processed on behalf of MoneyGram" (FAC ¶ 101) is equivalent to its allegation that Capgemini breached the MSA by "fail[ing] to use a degree of care as was appropriate to avoid unauthorized access, use or disclosure [of Customer Personal Data]." (*Id.* ¶ 76) Indeed, MoneyGram's allegation that Capgemini "stored and processed [the personal data] on behalf of MoneyGram" is a concession that the "duty to exercise reasonable care" is imposed by contract, not law. (*Id.* ¶ 101) This is further reinforced by the fact that the negligence claim arises from the exact same conduct as the breach of contract claim – the alleged failure of a Capgemini's Service Desk employee to follow authentication protocols when the Criminal Third Party called the Service Desk, and the subsequent disclosure of MoneyGram's Customer Personal Data by that Criminal Third Party. (*Compare id.* ¶ 74 *with id.* ¶ 104)

MoneyGram nonetheless attempts to add boilerplate allegations regarding a "special relationship" between itself and Capgemini relating to the handling of data to support the existence of duties separate from the MSA. (*Id.* ¶ 103) However, the FAC is devoid of any facts to support the existence of such a relationship. Furthermore, Texas law recognizes a special relationship sufficient to support an independent tort claim only "in certain limited contexts, such as where there exists an imbalance of bargaining power." *Popp v. New Residential Mortg., LLC*, 2022 WL 17824970, at *4-5 (S.D. Tex. Dec. 20, 2022) (dismissing negligence claim in light of economic loss doctrine). This doctrine "does not extend to ordinary commercial contractual relationships." *Adolph Coors Co. v. Rodriguez*, 780 S.W.2d 477, 481 (Tex. App. 1989), *writ denied* (Nov. 14, 1990) (holding that because plaintiff's injuries "consisted merely of economic loss . . . [defendant's] conduct does not give rise to an independent negligence cause of action"); *see also Johnson*, 999 F.Supp.2d at 931 (negligence claim barred by economic loss doctrine where "Plaintiff does not allege any facts to support the existence of a special relationship with Defendants"). Here, because MoneyGram and Capgemini are sophisticated business entities whose relationship arose from a detailed contract allocating their responsibilities and risks, MoneyGram cannot allege a special relationship sufficient to support an independent negligence claim.

Finally, the only injury that MoneyGram alleges is "the economic loss to the subject of [the agreements themselves]." *Jim Walter Homes*, 711 S.W.2d at 618. MoneyGram attempts to distinguish its negligence claim by tacking on additional alleged injuries such as "business interruption," "decreased business value," and "harm to reputation." (FAC ¶ 107) However, these injuries are insufficient to avoid the economic loss rule as a matter of law. *See Campbell v. ACProducts, Inc.*, 2022 WL 806611, at *5 (E.D. Tex. Feb. 25, 2022), *report and recommendation*

adopted, 2022 WL 798051 (E.D. Tex. Mar. 15, 2022) (dismissing negligence claim under economic loss doctrine and rejecting plaintiff's argument that "litigation costs and time spent litigating . . . and loss of business reputation" amounted to "damages outside" the contract); *Herman Cronier & Sons, Inc. v. Carrier Corp.*, 2013 WL 12090326, at *6 (S.D. Miss. Sept. 6, 2013) (dismissing negligence claim under economic loss doctrine and noting that "[i]t is immaterial that [plaintiff] seeks monetary relief for purported damage to its 'business reputation, labor costs, and business losses' . . . as these are also purely economic losses" (citing *E. River S.S. Corp. v. Transamerica Delaval, Inc.*, 476 U.S. 858, 870 (1986) (holding lost profits were purely economic); *Black's Law Dictionary* (9th ed. 2009) (including lost wages and profits and loss of goodwill and business reputation in definition of "economic loss")).

2. Capgemini's Actions Were Not The Proximate Cause Of MoneyGram's Damages

Finally, for the same reasons discussed above in connection with the breach of contract claim, MoneyGram's negligence claim should also be dismissed for lack of causation. MoneyGram's alleged injuries – stemming from third-party criminal conduct occurring within MoneyGram's own systems – are too remote, speculative, and attenuated to support liability. (*See* p. 16, *supra*) Moreover, the chain of causation from Capgemini's alleged conduct to MoneyGram's alleged injuries was broken by superseding criminal actions by third parties. (*See id.*); *Barton v. Whataburger, Inc.*, 276 S.W.3d 456, 462 (Tex. App.—Houston [1st Dist.] 2008) ("As a general rule, a person has no legal duty to protect another from the criminal acts of a third person. This is because the criminal conduct of a third party is a superseding cause that extinguishes any liability of the previous actor." (quotations and citations omitted)). The indirect and unforeseeable causal chain alleged here precludes recovery.

CONCLUSION

For the foregoing reasons, Capgemini respectfully requests that the Court dismiss the FAC in its entirety.

Dated: July 10, 2025

Respectfully submitted,

By: /s/ *Jeffrey M. Tillotson*
Jeffrey M. Tillotson
State Bar No. 20039200
J. Austen Irrobali
State Bar No. 24092564
TILLOTSON JOHNSON & PATTON
1201 Main Street, Suite 1300
Dallas, Texas 75202
Telephone: (214) 382-3041
Facsimile: (214) 292-6564
Email: jtillotson@tillotsonlaw.com
airrobali@tillotsonlaw.com

Jenny H. Kim (*pro hac vice*)
Jack G. Tubio (*pro hac vice*)
BOIES SCHILLER FLEXNER LLP
55 Hudson Yards
New York, New York 10001
Telephone: (212) 446-2354
Email: jkim@bsfllp.com
jtubio@bsfllp.com

Counsel for Defendant Capgemini America, Inc.

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document was electronically filed with the Court of the Clerk on July 10, 2025, using CM/ECF, which will send notification to the registered attorneys of record that the documents have been filed and are available for viewing and downloading.

/s/ *Jeffrey M. Tillotson*
Jeffrey M. Tillotson